National Security Cyber Assistance Program

The growing sophistication and number of cyber attacks necessitates an equally vigorous and rapid response. In exploring available approaches, the NSA developed a strategy to leverage the cyber expertise of industry. This newly formed strategic initiative is called the *National Security Cyber Assistance Program or NSCAP*.

NSCAP was designed around four pillars:

- Intrusion Detection
- Incident Response
- Vulnerability Assessment
- Penetration Testing

Each pillar will be incorporated into an accreditation framework for evaluating the capability of commercial cyber assistance service providers against industry best practices and NSA-developed criteria.



Objectives of the NSCAP accreditation include:

- Develop a list of "accredited" cyber service providers from which the NSS community can draw upon for timely cyber assistance.
- Promote public-private collaboration
- Leverage industry expertise to protect national interests
- Address this growing concern across government.

National Security Cyber
Assistance Program Office

E-mail: NSCAP@nsa.gov Website: http://www.nsa.gov/ia







Cyber Incident Response Assistance

Cyber Incident Response Assistance (CIRA) is the first accreditation of this strategic initiative. CIRA accreditation will be granted to qualified providers that are capable of consistently delivering CIR assistance to owners and operators of National Security Systems (NSS) as characterized by the 21 critical focus areas of CIRA.

Business Statement of Intent Service Agreement Log Collection and Analysis Core Capabilities Overview Client Engagement Management Process Network Traffic Data Collection and Analysis Process and Procedures **Communication Management Process** Host Integrity Data Collection and Analysis Staff Skill Documentation **Preliminary Data Collection** Incident Analysis CIRA Education and Training Plan Engagement Tools and Resources Identification Containment and Remediation Past Performance **Travel Management Process** Post-Incident Analysis

Client Furnished Information and Data
Rules of Engagement
Lessons Learned

National Security Cyber Assistance Program

Designed to meet the growing cyber defense needs of the U.S. government. Accreditation is issued to qualified Cyber Incident Response Providers capable of providing comprehensive cyber assistance services to owners/operators of National Security Systems.

Accredited Cyber Incident Service Providers

- Undergo a thorough review of their ability to deliver 21 focused areas of Incident Response Assistance services derived from industry best practices.
- Deliver consistent services using repeatable processes/procedures.
- Assign highly skilled and qualified staff to follow approved processes and procedures to deliver state-ofthe-art services.
- Improve quality of delivered services through training, lessons learned and shared situational awareness.



National Security System Owners/Users

- Use of an accredited cyber assistance provider instills confidence that highly capable resources are available when needed.
- Pre-established agreements with accredited providers fosters rapid engagement while minimizing response times and incident impact.
- Accredited Providers augment existing IR resources with specialized capabilities and tools as part of a comprehensive IA risk management program.
- Receive state-of-the-art Cyber Incident Response Assistance.